CLAIMS

What is claimed is:

1. A method for certifying pieces of data in a system with at least two levels of authorities, comprising the steps of:

(a) presenting a piece of data requiring certification to a first level authority for inspection of a given property;

(b) if the piece of data passes the inspection of the first level authority, causing a higher authority to receive an indication that the piece of data has passed the inspection of at least the first level authority;

(c) having the higher authority issue a certificate that the piece of data possesses the given property, the certificate including a signature of the higher authority but not including a public key of the first level authority; and

(d) storing information in order to keep at least the first level authority accountable for pieces of data that the first level authority contributes to certify.

2. A method for certifying, according to claim 1, wherein the piece of data presented is a public key having at least one corresponding secret key associated therewith.

3. A method for certifying, according to claim 2, wherein the given property of the public key includes a given user choosing

the public key to be used in connection with at least one of: a digital signature system and a public key encryption system.

4. A method for certifying, according to claim 3, wherein the inspection by the first level authority includes identifying the presenting user.

5. A method for certifying, according to claim 4, wherein the inspection includes verifying that the user knows the secret key that corresponds to the public key.

6. A method for certifying, according to claim 5, wherein the inspection includes checking a digital signature of a given message signed by the user relative to said public key, to determine that the user knows the secret key associated with the public key.

7. A method for certifying, according to claim 5, wherein the inspection includes verifying that the user knows the secret key associated with the public key by having the user decrypt a given message that is encrypted using the public key.

8. A method for certifying, according to claim 1, wherein a certified public verification key of the higher authority is sufficient to verify the certificate.

9. A method for certifying, according to claim 1, wherein the piece of data is included in the certificate.

10. A method for certifying, according to claim 9, wherein the higher authority contributes additional data that is included in the certificate.

11. A method for certifying, according to claim 1, wherein the information that is stored can be used to identify the first level authority.

12. A method for certifying, according to claim 11, wherein the information that is stored is a digital signature of the first level authority.

13. A method for certifying, according to claim 11, wherein the information that is stored indicates the name of the first level authority.

14. A method for certifying, according to claim 1, wherein at least a portion of the information that is stored is stored in the certificate.

15. A method for certifying, according to claim 14, wherein all of the information that is stored is stored in the certificate.

16. A method for certifying, according to claim 1, wherein the certificate includes a digital signature of the first level authority.

17. A method for certifying, according to claim 11, wherein the certificate includes a digital signature of the first level authority.

18. A method for certifying, according to claim 12, wherein the certificate includes a digital signature of the first level authority.

19. A method for certifying, according to claim 1, further comprising the step of:

(e) the higher level authority causes additional information to be saved which, when combined with the information that is stored, proves that the first level authority contributed to certification of the piece of data.

20. A method for certifying, according to claim 1, further comprising the step of:

(e) a witness causing information to be saved that indicates that the first level authority contributed to certification of the piece of data, wherein the information that is stored is stored in a way to indicate the identity of the witness.

21. A method for certifying, according to claim 20, wherein the information caused to be saved by the witness includes a portion of a digital signature and the information that is stored includes an other portion of a digital signature.

22. A method for certifying, according to claim 21, wherein the portions of the digital signature can be combined to prove that the first level authority contributed to certification of the piece of data.

23. A method for certifying public keys where there are a plurality of authorities A_1, . . ., A_n, where each i<n authority A_i can send authority A_{i+1} authenticated messages so that at least A_{i+1} can be sure that these messages genuinely come from A_i, and authority A_n has a signing key SK_n and an associated certified public key, PK_n, the method comprising the steps of:

(a) having a verification key PK_U presented to authority A_1;

(b) having authority A_1 verify, by means of a predetermined procedure, that PK_U possesses some properties out of a set of given properties;

(c) for all i<n, having authority A_i send authority A_{i+1} a message indicating that PK_U has been verified to possess the given properties;

(d) having A_n issue a certificate for PK_U, the certificate including a signature provided using SK_n but not including a public key of at least one authority A_j for some j<n; and

(e) storing information to keep A_j accountable for keys that A_j contributes to certify.

24. A method for certifying, according to claim 23, wherein the certificate does not include a public key of at least one other authority A_k.

25. A method for certifying, according to claim 24, wherein the certificate does not include public keys of any authorities A_1, A_2 . . . A_{n-2}, A_{n-1}.

26. A method for certifying, according to claim 25, wherein the certificate does not include a public key for A_n.

27. A method for certifying, according to claim 25, wherein the certificate includes a public key for A_n.

28. A method for certifying, according to claim 23, wherein knowledge of PK_n is sufficient to verify the certificate.

29. A method for certifying, according to claim 23, wherein PK_U is included in the certificate.

30. A method for certifying, according to claim 29, wherein at least one authority A_i, i<n, contributes additional data that is included in the certificate.

31. A method for certifying, according to claim 30, wherein all authorities contribute additional data that is included in the certificate.

32. A method for certifying, according to claim 23, wherein a digital signature of A_j is included in the certificate.

33. A method for certifying, according to claim 32, wherein digital signatures of all of the authorities are included in the certificate.

34. A method for certifying, according to claim 23, wherein for all i<n, authority A_i sends authority A_{i+1} a digital signature of A_i.

35. A method for certifying, according to claim 34, wherein for all i<n, authority A_i sends authority A_{i+1} a digital signature of A_i along with digital signatures of all previous authorities A_{i-1}, A_{i-2} . . . A_1.

36. A method for certifying, according to claim 35, wherein digital signatures of all of the authorities are included in the certificate.

37. A method for certifying, according to claim 23, wherein the information that is stored can be used to identify A_j.

38. A method for certifying, according to claim 37, wherein the information that is stored is a digital signature of A_j.

22

39. A method for certifying, according to claim 37, wherein the information that is stored indicates the name of A_j.

40. A method for certifying, according to claim 23, wherein at least a portion of the information that is stored is stored in the certificate.

41. A method for certifying, according to claim 40, wherein all of the information that is stored is stored in the certificate.

42. A method for certifying, according to claim 23, further comprising the step of:

(f) an authority A_k causing additional information to be saved which, when combined with the information that is stored, proves that A_j contributed to the certification of PK_U.

43. A method for certifying, according to claim 42, wherein k>j.

44. A method for certifying, according to claim 23, further comprising the step of:

(f) a witness causing information to be saved that indicates that A_j contributed to the certification of PK_U, wherein the information that is stored indicates the identity of the witness.

23

45. A method for certifying, according to claim 44, wherein the information that is caused to be saved by the witness includes a portion of a digital signature and the information that is stored includes an other portion of a digital signature.

46. A method for certifying, according to claim 45, wherein the portions of the digital signature can be combined to prove that A_j contributed to the certificate being issued.